PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-244547
(43)Date of publication of application : 08.09.2000

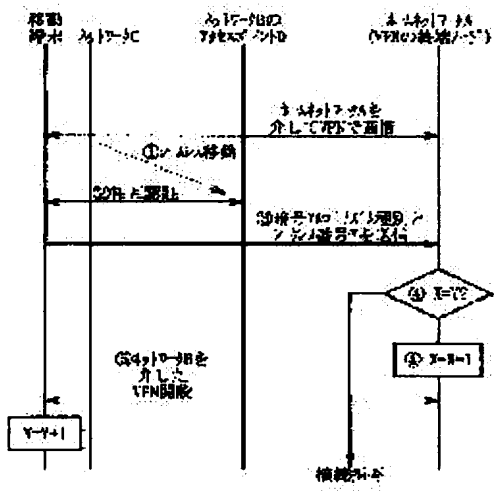
(51)Int.Cl. H04L 12/46
H04L 12/28
G09C 1/00
H04L 9/14
H04L 9/32
H04L 12/66

(21)Application number : 11-039196
(22)Date of filing : 17.02.1999

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : KUNO YUTAKA
HANAZAWA TETSUO
MORIKURA MASAHIRO

(54) CERTIFICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To select a suitable encription algorithm even when access to a home network is continued while moving between different types of networks.
SOLUTION: On the basis of network information reported from an access network B, a mobile terminal judges the strength of a required cipher and select the encription algorithm. Afterwards, at the time of certification with the tunnel server of a home network A, the mobile terminal sends the class of the selected encription algorithm and information capable of specifying this session while signing with the signature key thereof. The tunnel server verifies that signature and after the information capable of specifying this session reported from the mobile terminal is collated with information capable of specifying this session managed by the tunnel server, enciphered VPN communication based on the selected encription algorithm is started.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－244547
（P2000－244547A）
(43)公開日　平成12年９月８日(2000.9.8)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)	
Ｈ０４Ｌ	12/46		Ｈ０４Ｌ	11/00	３１０Ｃ	５Ｊ１０４
	12/28		Ｇ０９Ｃ	1/00	６６０Ｅ	５Ｋ０３０
Ｇ０９Ｃ	1/00	６６０	Ｈ０４Ｌ	9/00	６４１	５Ｋ０３３
Ｈ０４Ｌ	9/14				６７１	９Ａ００１
	9/32			11/20	Ｂ	

審査請求　未請求　請求項の数６　ＯＬ　（全　６　頁）　最終頁に続く

(21)出願番号　特願平11－39196

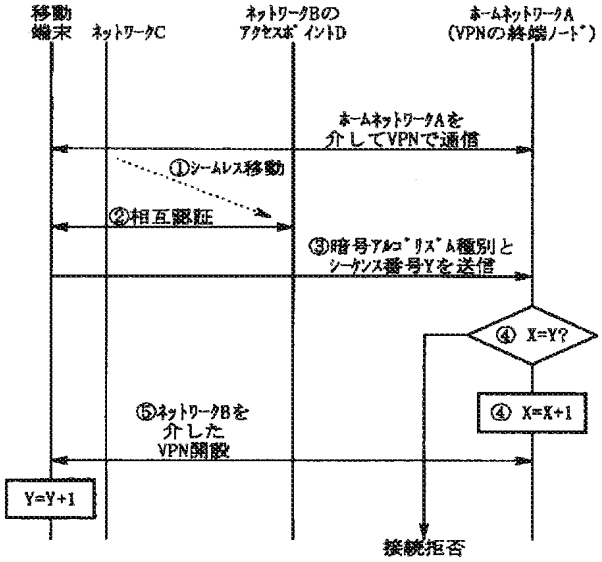
(22)出願日　平成11年２月17日(1999.2.17)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　久埜　豊
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　花澤　徹郎
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100064908
弁理士　志賀　正武

最終頁に続く

(54)【発明の名称】　認証方法

(57)【要約】
【課題】　異種ネットワーク間で移動しながらホームネットワークへのアクセスを継続しても、適切な暗号化アルゴリズムを選択できること。
【解決手段】　移動端末は、アクセスネットワークＢより通知されたネットワーク情報に基づいて、必要な暗号の強度を判断して、暗号化アルゴリズムを選択する。その後、移動端末は、ホームネットワークＡのトンネルサーバーとの認証時に、選択された暗号化アルゴリズムの種別と今回のセッションを特定しうる情報とを、自分の署名鍵で署名して送出する。トンネルサーバーは、該署名を検証し、移動端末より通知された今回のセッションを特定しうる情報とトンネルサーバーが管理している今回のセッションを特定しうる情報とを照合した上で、選択された暗号化アルゴリズムによる暗号化されたＶＰＮ通信を開始する。



1

【特許請求の範囲】

【請求項１】　移動端末、アクセスネットワーク、中継ネットワーク、ホームネットワーク及びホームネットワーク内のトンネルサーバーから構成され、
移動端末は、アクセスネットワークと中継ネットワークとを経由して、トンネルサーバーとの間で認証を行い、
移動端末とトンネルサーバーとの間で暗号化トンネルを開設して通信を行う通信システムの認証方法において、
移動端末は、
アクセスネットワークとの接続時に認証を行い、
アクセスネットワークとの認証時に、アクセスネットワークより通知されたネットワーク情報に基づいて、必要な暗号の強度を判断して、暗号化アルゴリズムを選択し、
トンネルサーバーとの認証時に、選択された暗号化アルゴリズムの種別と今回のセッションを特定しうる情報とを、自分の署名鍵で署名して送出し、
トンネルサーバーは、
前記署名を検証し、
移動端末より通知された今回のセッションを特定しうる情報とトンネルサーバーが管理している今回のセッションを特定しうる情報との照合結果に基づいて、移動端末の正当性を判定し、
正当性が認識されると、選択された暗号化アルゴリズムによる暗号化されたＶＰＮ通信を開始することを特徴とする認証方法。

【請求項２】　請求項１記載の認証方法において、
前記今回のセッションを特定しうる情報として、移動端末の外部からのアクセス回数を用いることを特徴とする認証方法。

【請求項３】　請求項１記載の認証方法において、
前記今回のセッションを特定しうる情報として、セッションの行われた時刻情報を用いることを特徴とする認証方法。

【請求項４】　移動端末、アクセスネットワーク、中継ネットワーク、ホームネットワーク及びホームネットワーク内のトンネルサーバーから構成され、
移動端末は、アクセスネットワークと中継ネットワークとを経由して、トンネルサーバーとの間で認証を行い、
移動端末とトンネルサーバーとの間で暗号化トンネルを開設して通信を行う通信システムの認証方法において、
移動端末は、
アクセスネットワークとの接続時に認証を行い、
トンネルサーバーとの認証時に、今回のセッションを特定しうる情報とアクセスネットワークとの認証時にアクセスネットワークより通知されたネットワーク情報とを、自分の署名鍵で署名して送出し、
トンネルサーバーは、
前記署名を検証し、
移動端末より通知された今回のセッションを特定しうる情報とトンネルサーバーが管理している今回のセッションを特定しうる情報との照合結果に基づいて、移動端末の正当性を判定し、
正当性が認識されると、移動端末より通知されたネットワーク情報に基づいて、必要な暗号の強度を判断して、暗号化アルゴリズムを選択し、
選択された暗号化アルゴリズムによる暗号化されたＶＰＮ通信を開始することを特徴とする認証方法。

【請求項５】　請求項４記載の認証方法において、
前記今回のセッションを特定しうる情報として、移動端末の外部からのアクセス回数を用いることを特徴とする認証方法。

【請求項６】　請求項４記載の認証方法において、
前記今回のセッションを特定しうる情報として、セッションの行われた時刻情報を用いることを特徴とする認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、異種ネットワーク間でシームレス移動を行いながらホームネットワークへアクセスする場合における認証方法に関する。

【０００２】

【従来の技術】近年、モバイル・コンピューティングの進展に従い、ファイアウォール（firewall）を越えて、自分が平常アクセスしているオフィスのネットワークに、外部からアクセスするＶＰＮ（Virtual Private Network）技術が発展を見ている。ＶＰＮの根幹は、ファイアウォール内にあるトンネルサーバーによる認証と暗号化トンネルの開設である。

【０００３】図３は、ＶＰＮを開設しながら、移動端末がアクセスネットワーク（構内ネットワーク）Ｂ，Ｃを介してホームネットワークＡに外部からアクセスを行うシステムの概要例を示す説明図である。この図において、ファイアウォールは、トンネルサーバーとの認証パケット、及び、トンネルサーバーとの暗号化トンネルを通るパケットのみを通すように設定されている。

【０００４】暗号化トンネルの開設は、以下の手順①～③で行われる（図４参照）。
①移動端末とトンネルサーバーとは、認証を行う（２－ａ）。
②暗号鍵のネゴシエーションを行う（２－ｂ）。
③暗号化トンネルを開設する（２－ｃ）。

【０００５】また、一般に、暗号解読にかかる所要時間は、単位時間当たりの暗号化試行回数によって決まるため、暗号化試行速度の速い暗号ほど短時間で解読されやすい傾向がある。図５は、暗号化アルゴリズムの特性（強度・速度）とネットワークとの関係を示す図表である。この表に示すように、専用線を介した接続の場合、及び、構内ネットワークを介した接続の場合には、高い安全性は要求されないが、上記専用線や上記構内ネット

ワークが有する高い伝送速度を低下させないためにも、高速度の暗号化アルゴリズムが要求される。一方、インターネットを介した接続の場合には、伝送路（インターネット）自体の伝送速度が低いと考えられるため、高速度の暗号化アルゴリズムは要求されないが、高い安全性が要求される。

【０００６】実際に現在市販されているＶＰＮシステムとしては、（１）主に構内ネットワークにおいて使用されることを念頭におき、簡易暗号を使用しているシステム、（２）ＯＣＮ等の商用インターネットサービスにおいて使用されることを念頭におき、強い暗号を使用しているシステムなどがある。上記（１）の一例としては、Logical Office（谷本他、”ロジカルオフィスサービス”、ＮＴＴ　Ｒ＆Ｄ、Vol.45　No.10　１９９６年）がある。また、上記（２）の一例としては、ＤＥＣ，ＮＴＴ－ＡＴ社製 Altavista tunnel がある。

【０００７】

【発明が解決しようとする課題】ところで、近年標準化の進展が著しい無線ＬＡＮの新しい利用形態として、異種ネットワーク間にまたがって、移動しながら継続した通信を行っていく通信形態が現実のものとなってきている。該利用形態の一例としては、図３に示すように、移動端末の移動に伴って、通信を介するアクセスネットワークをアクセスネットワークＣからアクセスネットワークＢに変更することが考えられる。このような利用形態においては、移動端末とホームネットワークとの間における暗号化トンネルが様々な通信経路を経由することになる。

【０００８】そのため、従来のシステム（単一の暗号化アルゴリズムしか用意されていないシステム）では、該用意された暗号化アルゴリズムが、現在経由している通信経路に対して、必要以上に安全であるが要求される処理速度を満たしていない場合であっても、または、必要以上に高速であるが要求される安全性を満たしていない場合であっても、該用意された暗号化アルゴリズムを使用せざるを得ない、という課題があった。

【０００９】この発明は、このような背景の下になされたもので、異種ネットワーク間でシームレス移動を行いながらホームネットワークへのアクセスを継続しても、必要な強度・速度の暗号化アルゴリズムを適切に選択することができる認証方法を提供することを目的とする。

【００１０】

【課題を解決するための手段】請求項１記載の発明は、移動端末、アクセスネットワーク、中継ネットワーク、ホームネットワーク及びホームネットワーク内のトンネルサーバーから構成され、移動端末は、アクセスネットワークと中継ネットワークとを経由して、トンネルサーバーとの間で認証を行い、移動端末とトンネルサーバーとの間で暗号化トンネルを開設して通信を行う通信システムの認証方法において、移動端末は、アクセスネットワークとの接続時に認証を行い、アクセスネットワークとの認証時に、アクセスネットワークより通知されたネットワーク情報に基づいて、必要な暗号の強度を判断して、暗号化アルゴリズムを選択し、トンネルサーバーとの認証時に、選択された暗号化アルゴリズムの種別と今回のセッションを特定しうる情報とを、自分の署名鍵で署名して送出し、トンネルサーバーは、前記署名を検証し、移動端末より通知された今回のセッションを特定しうる情報とトンネルサーバーが管理している今回のセッションを特定しうる情報との照合結果に基づいて、移動端末の正当性を判定し、正当性が認識されると、選択された暗号化アルゴリズムによる暗号化されたＶＰＮ通信を開始することを特徴とする。請求項２記載の発明は、請求項１記載の認証方法において、前記今回のセッションを特定しうる情報として、移動端末の外部からのアクセス回数を用いることを特徴とする。請求項３記載の発明は、請求項１記載の認証方法において、前記今回のセッションを特定しうる情報として、セッションの行われた時刻情報を用いることを特徴とする。請求項４記載の発明は、移動端末、アクセスネットワーク、中継ネットワーク、ホームネットワーク及びホームネットワーク内のトンネルサーバーから構成され、移動端末は、アクセスネットワークと中継ネットワークとを経由して、トンネルサーバーとの間で認証を行い、移動端末とトンネルサーバーとの間で暗号化トンネルを開設して通信を行う通信システムの認証方法において、移動端末は、アクセスネットワークとの接続時に認証を行い、トンネルサーバーとの認証時に、今回のセッションを特定しうる情報とアクセスネットワークとの認証時にアクセスネットワークより通知されたネットワーク情報とを、自分の署名鍵で署名して送出し、トンネルサーバーは、前記署名を検証し、移動端末より通知された今回のセッションを特定しうる情報とトンネルサーバーが管理している今回のセッションを特定しうる情報との照合結果に基づいて、移動端末の正当性を判定し、正当性が認識されると、移動端末より通知されたネットワーク情報に基づいて、必要な暗号の強度を判断して、暗号化アルゴリズムを選択し、選択された暗号化アルゴリズムによる暗号化されたＶＰＮ通信を開始することを特徴とする。請求項５記載の発明は、請求項４記載の認証方法において、前記今回のセッションを特定しうる情報として、移動端末の外部からのアクセス回数を用いることを特徴とする。請求項６記載の発明は、請求項４記載の認証方法において、前記今回のセッションを特定しうる情報として、セッションの行われた時刻情報を用いることを特徴とする。

【００１１】

【発明の実施の形態】§１．概要

本発明は、アクセスネットワークへの接続時に、移動端末とアクセスネットワークとが相互認証を行い、該アクセスネットワークに関する情報（ネットワークアドレ

5

ス，運用機関の情報）を得て、該情報に基づいて、必要な強度・速度の暗号化アルゴリズムを選択することを、最も主要な特徴とする。移動端末が異種ネットワーク間をまたがる移動をしながら、各時点で最も適切な暗号化アルゴリズムを選択して通信を行える点が、従来技術とは異なる。本発明によると、接続するネットワークに応じて、求められる安全性・速度を判断して、適切な暗号化アルゴリズムを選択することが可能であり、特に、無線ＬＡＮ等の高度移動通信システムにおいて、常に自分のオフィス環境にアクセスし続けることを可能とする効果が得られる。

【００１２】§２．第１実施形態

以下、図面を参照して、この発明の第１実施形態について説明する。なお、本実施形態は請求項２に対応するが、以下の説明において、「回数情報」を「時刻情報」と置き換えることによって請求項３に対応する説明となり、また、「回数情報」を「今回のセッションを特定しうる情報」と置き換えることによって請求項１に対応する説明となる。

【００１３】図１は、この発明の第１実施形態による認証方法の一例を示すシーケンス図である。この図では、初期状態として、図３のように、「移動端末が、アクセスネットワークＣを介して、ホームネットワークＡとＶＰＮ暗号化トンネルを開設し、通信を行っている」場合を考える。

【００１４】この初期状態において、移動端末が図３のように移動すると、通信に使用されるアクセスネットワークは、アクセスネットワークＣからアクセスネットワークＢに切り替わる。アクセスネットワークＢに切り替わると、移動端末とアクセスネットワークＢとは、公開鍵証明書を相互認証する。

【００１５】移動端末は、アクセスネットワークＢとの相互認証時に、アクセスネットワークＢの証明書中のネットワーク情報に基づいて、アクセスネットワークＢに適した暗号化アルゴリズムを選択する。

【００１６】移動端末は、選択された暗号化アルゴリズムの種別を示す暗号化アルゴリズム選択メッセージに対して、該移動端末固有の署名鍵で署名し、署名された暗号化アルゴリズム選択メッセージを、ホームネットワークＡのＶＰＮの終端ノード（トンネルサーバー）に送出する。

【００１７】このとき、移動端末は、（この署名された暗号化アルゴリズム選択メッセージを解析することによって求められる）上記署名鍵がアクセスネットワークＢによって流用されることを防がなくてはならない。そこで、移動端末は、外部からホームネットワークＡにアクセスした回数を示す回数情報を、被署名文（即ち、暗号化アルゴリズム選択メッセージ）に組み込み、この回数情報が組み込まれた暗号化アルゴリズム選択メッセージに対して署名する。これによると、アクセスネットワークＢは回数情報を偽造できないので、署名鍵を解析・流用することも不可能となる。

6

【００１８】回数情報が組み込まれた後に署名された暗号化アルゴリズム選択メッセージを受信すると、ホームネットワークＡは、該受信内容から回数情報（即ち、移動端末が管理している回数情報、以下、「移動端末側回数情報」と称する）を取り出し、該移動端末側回数情報を、移動端末からホームネットワークＡへのアクセスに関してホームネットワークＡが管理している回数情報（以下、「ホームネットワーク側回数情報」と称する）と照合する。

【００１９】もし、移動端末側回数情報とホームネットワーク側回数情報とが一致しないならば、ホームネットワークＡは、移動端末との接続を拒否し、処理は終了する。一方、移動端末側回数情報とホームネットワーク側回数情報とが一致するならば、ホームネットワークＡは、ホームネットワーク側回数情報（が示す回数）を１増やす。

【００２０】ホームネットワークＡは、回数情報が組み込まれた後に署名された暗号化アルゴリズム選択メッセージから暗号化アルゴリズム選択メッセージを取り出し、該暗号化アルゴリズム選択メッセージが示す種別の暗号化アルゴリズム（即ち、移動端末によって選択された暗号化アルゴリズム）に基づいて、ＶＰＮ暗号化トンネルを開設する。最後に、移動端末は、移動端末側回数情報（が示す回数）を１増やす。以上で、処理は終了する。

【００２１】上記の認証方法によれば、異種ネットワーク間でシームレス移動を行いながらホームネットワークへのアクセスを継続しても、必要な強度・速度の暗号化アルゴリズムを適切に選択することができる。

【００２２】§３．第２実施形態

以下、図面を参照して、この発明の第２実施形態について説明する。なお、本実施形態は請求項５に対応するが、以下の説明において、「回数情報」を「時刻情報」と置き換えることによって請求項６に対応する説明となり、また、「回数情報」を「今回のセッションを特定しうる情報」と置き換えることによって請求項４に対応する説明となる。

【００２３】図２は、この発明の第２実施形態による認証方法の一例を示すシーケンス図である。この図でも、初期状態として、図３のように、「移動端末が、アクセスネットワークＣを介して、ホームネットワークＡとＶＰＮ暗号化トンネルを開設し、通信を行っている」場合を考える。

【００２４】この初期状態において、移動端末が図３のように移動すると、通信に使用されるアクセスネットワークは、アクセスネットワークＣからアクセスネットワークＢに切り替わる。アクセスネットワークＢに切り替わると、移動端末とアクセスネットワークＢとは、公開

7

鍵証明書を相互認証する。

【００２５】移動端末は、アクセスネットワークＢとの相互認証時に、アクセスネットワークＢの証明書中のネットワーク情報に対して、該移動端末固有の署名鍵で署名し、署名されたネットワーク情報を、ホームネットワークＡのＶＰＮの終端ノード（トンネルサーバー）に送出する。

【００２６】このとき、移動端末は、（この署名されたネットワーク情報を解析することによって求められる）上記署名鍵がアクセスネットワークＢによって流用されることを防がなくてはならない。そこで、移動端末は、外部からホームネットワークＡにアクセスした回数を示す回数情報を、被署名文（即ち、上記ネットワーク情報）に組み込み、この回数情報が組み込まれたネットワーク情報に対して署名する。これによると、アクセスネットワークＢは回数情報を偽造できないので、署名鍵を解析・流用することも不可能となる。

【００２７】回数情報が組み込まれた後に署名されたネットワーク情報を受信すると、ホームネットワークＡは、該受信内容から回数情報（即ち、移動端末側回数情報）を取り出し、該移動端末側回数情報を、移動端末からホームネットワークＡへのアクセスに関してホームネットワークＡが管理している回数情報（即ち、ホームネットワーク側回数情報）と照合する。

【００２８】もし、移動端末側回数情報とホームネットワーク側回数情報とが一致しないならば、ホームネットワークＡは、移動端末との接続を拒否し、処理は終了する。一方、移動端末側回数情報とホームネットワーク側回数情報とが一致するならば、ホームネットワークＡは、ホームネットワーク側回数情報（が示す回数）を１増やす。

【００２９】ホームネットワークＡは、回数情報が組み込まれた後に署名されたネットワーク情報からネットワーク情報を取り出し、該ネットワーク情報に基づいて、アクセスネットワークＢに適した暗号化アルゴリズムを選択する。ホームネットワークＡは、該選択された暗号化アルゴリズムに基づいて、ＶＰＮ暗号化トンネルを開設する。最後に、移動端末は、移動端末側回数情報（が

8

示す回数）を１増やす。以上で、処理は終了する。

【００３０】上記の認証方法によれば、異種ネットワーク間でシームレス移動を行いながらホームネットワークへのアクセスを継続しても、必要な強度・速度の暗号化アルゴリズムを適切に選択することができる。

【００３１】§４．捕捉

以上、この発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計の変更等があってもこの発明に含まれる。

【００３２】

【発明の効果】以上説明したように、この発明によれば、アクセスネットワークに関するネットワーク情報に基づいて暗号化アルゴリズムを選択することができるので、必要な安全性と処理速度とを備えた暗号化アルゴリズムを適切に選択することができる。特に、無線ＬＡＮを用いたモバイルコンピューティングにおいては、本発明により、シームレスに異種ネットワーク間を移動することができるようになる。また、「従来の技術」の項で説明したようなシステム（構内ネットワーク向けシステムと商用インターネット向けシステム）の２つを、ユーザーに購入させる必要が無くなるため、システムヴェンダーとしては、スケールメリットを享受できる。

【図面の簡単な説明】

【図１】　この発明の第１実施形態による認証方法の一例を示すシーケンス図である。

【図２】　この発明の第２実施形態による認証方法の一例を示すシーケンス図である。

【図３】　ＶＰＮを開設して通信を行うシステムの概要例を示す説明図である。

【図４】　暗号化トンネルを開設する手順の一例を示すシーケンス図である。

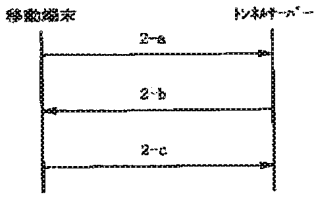
【図５】　暗号化アルゴリズムの特性（強度・速度）とネットワークとの関係を示す図表である。

【符号の説明】

Ａ……ホームネットワーク

Ｂ，Ｃ……アクセスネットワーク

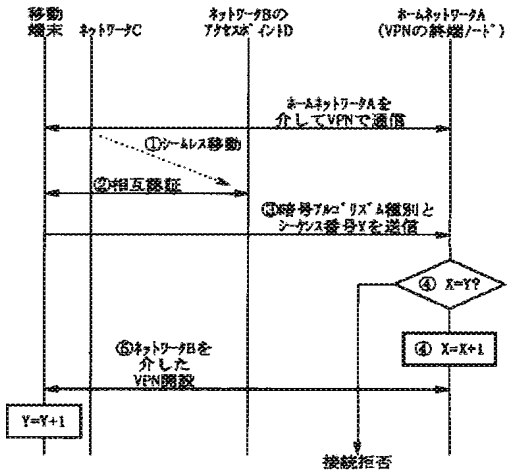
【図４】



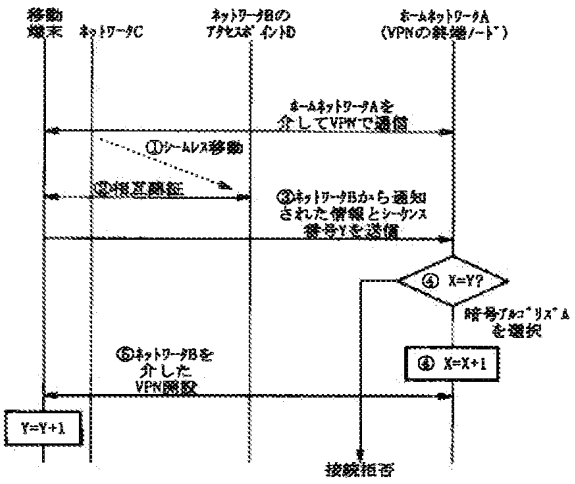
【図５】

	構内/専用線接続	インターネットを介した接続
強い暗号 (=遅い暗号)	適していない。	適している。
簡易暗号 (=弱い暗号)	適している。	適していない。

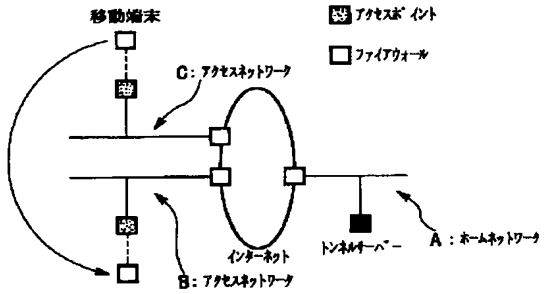
【図１】



【図２】



【図３】



フロントページの続き

(51) Int. Cl.[7]	識別記号	F I	テーマコード（参考）
H04L 12/66			

(72)発明者　守倉　正博
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

Ｆターム（参考）　5J104 AA07 AA35 AA36 KA02 KA10 NA38 PA01 PA07
5K030 GA15 JT09
5K033 AA08 DA19
9A001 CC05 CC06 EE03 JJ27 LL03